REMARKS

Reconsideration and further examination of the subject patent application in light of the present Amendment and Remarks is respectfully requested. Applicant has amended the claims, thereby making the pending rejections moot. However, to expedite prosecution, Applicant provides herein an explanation of how the claimed invention differs from the cited reference to Monroe '614.

Monroe relates to mainframe computers where access to the memory resources needs to be controlled in order to avoid one user interfering with the work of another user. Therefore, Monroe divides the memory into a plurality of hierarchical protection domain levels, wherein each object is contained in a protection domain and each task is executed in a protection domain (see, e.g., cl. 5, ln. 33-40). Monroe allows tasks operating in a high domain level to access objects in equal or lower domain levels, but disallows tasks executing in a specific domain level to access objects in a higher domain level. Therefore, Monroe assigns the basic operating system functions to the highest domain level, i.e., permitting access to all resources, but severely restricting access to other tasks (cl. 5, ln. 54-58). Conversely, the lowest level is intended for object to which all other resources should have access, but which receives the least protection.

As can be readily understood, such a scheme cannot be employed in a modern PC operating system, such as Windows®. For example, the Windows® operating system includes objects designated as DLL objects which, being part of the operating system, must receive the highest protection, but also must be accessible to every process running on the computer. Since DLL objects must be accessible to every process, using the Monroe scheme they can only be saved in the lowest domain, i.e., Monroe's common problem domain. However, saving the DLL objects in the common problem domain would expose the objects to any malicious code attack, as the common problem domain receives the lowest protection. Conversely, if one follows Monroe's proposal, the DLL object will be stored in the highest protection domain level to ensure their integrity. However, that would prevent access to the DLL objects by practically all other processes running on the computer – which would render it inoperable.

The presently claimed invention is designed to protect computers running modern operating systems, such as Windows®, from malicious code attacks. The claimed invention enables decoupling the access rights from the protection level applied to an object. To achieve that, the claimed invention assigns to each object a trust value and an object type and to each process a trust value. A set of rules is stored in the computer for each combination of object trust value, process trust value, and object type. In this manner, two objects having the same trust values may receive high protection, but access to these files by a process would depend not only on their trust value, but on the combination of trust value of the object, of the process, and on the object type. This feature is claim in, among others, claim 1, which is allowable over Monroe. To illustrate, in Monroe a process running in a low domain can never access an object residing in a higher domain. Conversely, according to the invention recited in claim 1, a process of low trust value may be granted access to an object of a higher trust value depending on the object type and the rule assigned to the combination of object type, object trust value, and process trust value. This enables, for example, assigning a high trust value to a DLL object, but designating its object type and the associated rule to enable access from lower trust value processes.

The subject invention provides other features that distinguish it from Monroe. For example, the feature of claim 6 relates to defining operation types and enhancing the decision granularity by including in the rules a dependency on the operation type of the access request from the process. This can provide immensely enhanced security feature. Turning to our DLL example, in order to provide the maximum security to the DLL objects, while allowing use of the DLL object by every process as required by the Windows® operating system, the trust value of the DLL object can be set to the highest and the rule can be set to allow access only for one specific operation type. Using the format of the subject specification, one can employ the following rules set to protect the DLL files, but allow the required access by program without allowing tempering with the DLL object.

- Assign highest trust value: 10
- assign target object type "executable"
- assign rules to each combination of process trust value lower than 10, object trust value 10 and object type "executable" with the various operation types: read, write, delete, open, modify, wherein:
    - the rule containing the operation type: write, delete or modify the rule would deny the access

- the rules containing the combinations: read or open, the rules would permit the access.

In this manner, every process requiring the DLL file will be able to access it even if it has a lower trust value, but no process will be able to damage the DLL objects as operation types associating with malicious code operations, i.e., write, delete, or modify, are not allowed by the respective rules. Such a scheme is not disclosed nor suggested by Monroe. Therefore, claim 6 is allowable over Monroe.

The remaining claims provide features that further distinguish the claimed invention from Monroe, or any other prior art of record.

For the foregoing reasons, applicant submits that the subject application is in condition for allowance and earnestly solicits an early Notice of Allowance. Should the Examiner be of the opinion that a telephone conference would expedite prosecution of the subject application, the Examiner is respectfully requested to call the undersigned at the below-listed number.

Applicant hereby petitions for any extension of time that may be required to keep this application alive.

Respectfully submitted,

TransPacific Law Group

By ______________________
Joseph Bach
Registration No. 37,771

April 23, 2005

TransPacific Law Group
17460 Lakeview Drive
Morgan Hill, CA 95037
(408) 623-9466
(408) 782-9931 fax
jbach@TransPacificLaw.com